UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/903,278	07/11/2001	Philip M. Walker	10012790-1	9299

22879 7590 04/23/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
TRAN, TONGOC	

ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
04/23/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte PHILIP M. WALKER and DAVID J. KRENITSKY

Appeal 2009-001183
Application 09/903,278
Technology Center 2100

Decided: April 21, 2010

Before JOSEPH L. DIXON, STEPHEN C. SIU, and JAMES R. HUGHES, *Administrative Patent Judges.*

DIXON, *Administrative Patent Judge.*

DECISION ON APPEAL

The Appellants appeal under 35 U.S.C. § 134(a) from the final rejection of claims 1-26. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

I. STATEMENT OF THE CASE

The Invention

The invention at issue on appeal relates to a method and system for detecting whether a system is altered (Spec. 1).

The Illustrative Claim

Claim 1, an illustrative claim, reads as follows:

> 1. A system comprising:
>
> a target;
>
> a probe operable to execute in the target and collect a predetermined set of data associated with the target; and
>
> a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered.

The References

The Examiner relies on the following references as evidence:

Schneier	US 5,978,475	Nov. 2, 1999
Hill	US 6,088,804	Jul. 11, 2000

The Rejections

Claims 1-17, 19-24, and 26 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Schneier.

Claims 1, 10, and 19 stand rejected under 35 U.S.C. § 102(e) as being

anticipated by Hill.

Claims 18 and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier.

Only those arguments actually made by the Appellants have been considered in this decision. Arguments which the Appellants could have made but chose not to make in the Briefs have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii) (2008).

II. ISSUES

Has the Examiner erred in finding that Schneier discloses "a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered," as recited in claim 1?

Has the Examiner erred in finding that Hill discloses "a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered," as recited in claim 1?

III. PRINCIPLES OF LAW

Scope of Claim

During prosecution before the USPTO, claims are to be given their broadest reasonable interpretation, and the scope of a claim cannot be narrowed by reading disclosed limitations into the claim. *See In re Morris*,

127 F.3d 1048, 1054 (Fed. Cir. 1997). The Office must apply the broadest reasonable meaning to the claim language, taking into account any definitions presented in the specification. *In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004) (citing *In re Bass*, 314 F.3d 575, 577 (Fed. Cir. 2002)).

"Giving claims their broadest reasonable construction 'serves the public interest by reducing the possibility that claims, finally allowed, will be given broader scope than is justified.'" *Id.* (quoting *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984)). "Construing claims broadly during prosecution is not unfair to the applicant . . . because the applicant has the opportunity to amend the claims to obtain more precise claim coverage." *Id.*

Anticipation

"[A]nticipation of a claim under § 102 can be found only if the prior art reference discloses every element of the claim . . . ." *In re King*, 801 F.2d 1324, 1326 (Fed. Cir. 1986) (citing *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick Co.,* 730 F.2d 1452, 1457 (Fed. Cir. 1984)). "[A]bsence from the reference of any claimed element negates anticipation." *Kloster Speedsteel AB v. Crucible, Inc.,* 793 F.2d 1565, 1571 (Fed. Cir. 1986).

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros., Inc. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). Analysis of whether a claim is patentable

over the prior art under 35 U.S.C. § 102 begins with a determination of the scope of the claim. We determine the scope of the claims in patent applications not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction in light of the Specification as it would be interpreted by one of ordinary skill in the art. *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d at 1364. The properly interpreted claim must then be compared with the prior art.

In rejecting claims under 35 U.S.C. § 102, "[a] single prior art reference that discloses, either expressly or inherently, each limitation of a claim invalidates that claim by anticipation." *Perricone v. Medicis Pharm. Corp.,* 432 F.3d 1368, 1375 (Fed. Cir. 2005) (citation omitted).

Obviousness

"Obviousness is a question of law based on underlying findings of fact." *In re Kubin*, 561 F.3d 1351, 1355 (Fed. Cir. 2009). The underlying factual inquiries are: (1) the scope and content of the prior art, (2) the differences between the prior art and the claims at issue, (3) the level of ordinary skill in the pertinent art, and (4) secondary considerations of nonobviousness. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (citation omitted).

IV. FINDINGS OF FACT

The following findings of fact (FFs) are supported by a preponderance of the evidence.

Schneier

1. Schneier discloses an event auditing system in which an untrusted computer 102 (target) contains a cryptographic module 165, an auditing program 200, and an audit log 300 with predetermined format (combined as a probe) in its storage 160 to be operable together to determine whether the audit log 300 as well as the untrusted computer 102 has been altered (Abstract; col. 3, ll. 7-52; Figs. 1-3).

2. Schneier further discloses that a verification step by a trusted machine or person consists of a plurality of operations on the audit log file for utilizing a MAC to determine whether it has been altered (col. 7, ll. 16-18, col.14, ll. 24-28):

To verify the desired subset:

> 1. At step 610, V goes through the log entries L_o to L_f, verifying that each entry Y_j in the hash chain is correct. Each hash chain entry Y_j=hash (Y_{j-1}, $E_{kj}(D_j)$, W_j) can be verified by using the hash chain, encrypted data, and log entry type values for the immediately preceding hash chain entry from its log entry value. The starting values W_o and E_{ko} (D_o) are known from L_o, and Y_o is known to be defined as a block of binary zeros. Thus, the hash chain entries can be verified recursively starting from information available in the sequence of accessible log entries.

(Col. 13, ll. 23-33).

> 8. At step 680, T forms and sends to V
>
> M_3=p, R[0..n].
>
> V is now able to decrypt, but not to change, the data in the log entries whose keys were sent in R. The verifier is also convinced that the log entries are validly MAC'd, since a correct MAC on any hash-chain value is essentially a MAC on all previous entries, as well.

(Col. 14, ll. 20-28).

Hill

3. Hill discloses a method and system for responding to the security attacks on a computer network. A SOM processor maps a vector representative of first training signature into display cell which is in the region of patterns of a display map to determine the type of security attack and the severity in a quick interpretable form. (Abstract; col. 7, ll. 1-8).

V. ANALYSIS

The Appellants have the opportunity on appeal to the Board of Patent Appeals and Interferences (BPAI) to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) (citing *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)). The Examiner sets forth a detailed explanation of a reasoned conclusion of unpatentability in the Examiner's Answer. Therefore, we look to Appellants' Briefs to show error therein.

Grouping of Claims

The Appellants have elected to argue claims 1-5, 7, 9-14, 19-24, and 26 together as a group for the Schneier reference (App. Br. 5-6). The Appellants have also elected to argue claims 1, 10, and 19 together as a group for the Hill reference (App. Br. 8-11). Therefore, we select independent claim 1 as the representative claim for both groups, and we will address the Appellants' arguments with respect thereto. 37 C.F.R. § 41.37(c)(1)(vii). *See also In re Nielson*, 816 F.2d 1567, 1572 (Fed. Cir. 1987).

35 U.S.C. § 102 rejection

We start our review by first determining the appropriate scope of the argued claim limitations in the independent claims.

The claims themselves do not define the argued terms. Therefore, we have an obligation to construe the terms broadly, yet reasonably. In light of the breadth of Appellants' Specification, we broadly, but reasonably construe the claimed "target" as any object that can be altered; the claimed "collected predetermined set of data" as any predetermined set of data; the claimed "expected data values" as any expected data values; and the claimed "probe" as any program or program module or the combination of program module and data set.

We now address the merits of the Appellants' contentions under our claim construction.

Schneier Reference

With respect to claim 1, the Appellants contend that "the *Schneier* reference appears to be directed toward determining whether the 'predetermined set of data' (the audit log 300) is altered, instead of whether the untrusted computer 102 of *Schneier* (the 'target') has been altered." (App. Br. 5-6).

We disagree with the narrow interpretation of the disputed claim terminology by the Appellants. We find that the audit log 300 is a part of the storage device 160 in the untrusted computer 102 (FF 1). Thus, altering the audit log is equivalent to altering the target, i.e., untrusted computer, under our above-noted claim construction.

The Appellants further contend that the audit log 300 of Schneier is not compared with expected values to determine whether the target has been altered because "the information of the audit log 300 . . . appears to be completely unexpected and/or random based on what acts or events happened to take place or occur with the computer of *Schneier*." (App. Br. 6; Reply Br. 5). "[T]he Examiner appears to consider either the verification data or the billing data to meet these limitations (Examiner's Answer, page 10). However, it is the verification data that is compared to expected values." (Reply Br. 5).

We disagree with the Appellant's contentions. First, under our claim construction, both "collected predetermined set of data" and "expected data values" should be interpreted broadly. We find Schneier teaches that the audit log collects and contains a set of log entry data with predetermined

format (FF 1). Thus, the collected set of data, regardless of the randomness of the entries, can be read on "collected predetermined set of data" as recited in claim 1. Furthermore, we find that the immediate preceding hash chain entry forms its log entry value or a message authentication code (MAC) on previous entries disclosed by Schneier (FF 2) can be read as "expected values." Moreover, we find Schneier teaches that the verifier V verifies the set of hash log entries by recursively using immediately preceding hash chain entry values (expected values) and compares the derived MAC to a MAC (expected value) on previous entries to determine whether the entry of the audit log is altered (FF 2). Finally, we note that the limitation of the verification data compares to expected values argued by the Appellants is not expressly recited in the language of independent claim 1.

Therefore, we find the Appellants have not met the requisite burden of providing evidence or argument to show error in the Examiner's finding of anticipation by Schneier for representative claim 1.

Accordingly, we sustain the Examiner's rejection of representative claim 1 as being anticipated by Schneier under 35 U.S.C. § 102. Independent claims 10 and 19 contain similar limitations, and the Appellants present similar arguments thereto. Therefore, we also sustain the Examiner's anticipation rejection of independent claims 10 and 19.

We also sustain the Examiner's anticipation rejection of dependent claims 2-5, 7, 9, 11-14, 17, 18, 20-24, and 26, which have not been separately argued. *See* 37 C.F.R. § 41.37(c)(1)(vii); *In re Nielson*, 816 F.2d at 1572.

With respect to claims 6, 8, 15, and 16, the Appellants contend that in Schneier, the audit logging program 200 (which the Examiner consider as corresponding to the "probe" recited in claim 6, 8, 15, and 16) does not calculate the signature value, and thus, Schneier does not teach or suggest the claimed limitations of the probe is operable to calculate a signature value. (App. Br. 7-8; Reply Br. 6-8).

We disagree with the Appellants' contention. As noted earlier, since the claims do not define the form of the probe, we construe the claimed probe as any combination of program, program module, and log of data. We further find Schneier teaches that in the untrusted computer 102, a probe consists of a cryptographic module 165, an auditing program 200, and an audit log 300 (FF 1). We also find that Schneier teaches that a signature value is calculated by the probe such as MAC (FF 2).

Therefore, we also sustain the Examiner's anticipation rejection of dependent claims 6, 8, 15, and 16.

Hill Reference

The Appellants also contend that Hill does not anticipate claim 1 because Hill is not making any comparison to determine whether the target has been altered (App. Br. 9; Reply Br. 9).

We agree with the Appellants' contention. We find that Hill only teaches determining the types of security attacks and the severity of the attacks (FF 3), not whether a node or the network has been altered. The Examiner does not indicate, and we do not readily find where the Hill

reference teaches determining whether the network or a node of the network has been altered.

Therefore, we find the Appellants have met the requisite burden of providing evidence or argument to show error in the Examiner's finding of anticipation by Hill for representative claim 1.

Accordingly, we cannot sustain the Examiner's rejection of representative claim 1 as being anticipated by Hill under 35 U.S.C. § 102. Independent claims 10 and 19 contain similar limitations, and the Appellants present similar arguments thereto. Therefore, we also cannot sustain the Examiner's anticipation rejection of independent claims 10 and 19 as being anticipated by Hill under 35 U.S.C. § 102.

35 U.S.C. § 103(a) rejection

We sustain the Examiner's obviousness rejections of dependent claims 18 and 25, which are not separately argued, and therefore, fall with their respective base claims. *See* 37 C.F.R. § 41.37(c)(1)(vii); *In re Nielson*, 816 F.2d at 1572.

CONCLUSION

Accordingly, based on our consideration of the totality of the record before us, we have weighed the evidence of anticipation found in the applied references, with the Appellants' countervailing evidence and arguments for non- anticipation by Schneier and conclude that the claimed invention encompassed by appealed claims 1-17, 19-24, and 26 would have been

unpatentable under 35 U.S.C. § 102(b) and claims 18 and 25 would have been unpatentable as a matter of law under 35 U.S.C. § 103(a).

However, we conclude that the Hill reference does not disclose "a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered," as recited in claim 1.

VII. DECISION

We affirm the anticipation rejection of claims 1-17, 19-24, and 26 by Schneier under 35 U.S.C. § 102(b).

We affirm the obviousness rejection of claims 18 and 25 over Schneier under 35 U.S.C. § 103(a).

We reverse the anticipation rejection of claims 1, 10, and 19 by Hill under 35 U.S.C. § 102(e).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

Appeal 2009-001183
Application 09/903,278

msc

HEWLETT-PACKARD COMPANY
INTELLECTUAL PROPERTY ADMINISTRATION
3404 E. HARMONY ROAD
MAIL STOP 35
FORT COLLINS CO 80528